International Journal of Experiential Learning & Case Studies
4 : 2 (December 2019) pp. 237-253. dx.doi.org/10.22555/ijelcs.v4i2.2543

ATM & BIOMETRIC SOLUTIONS: A CASE STUDY

Yamna Sheikh, Muhammad Imran Majid***

Abstract

The paper highlights security features for biometric systems along with application-specific to a bank in Pakistan. Further, a comprehensive view of retinal scanning and application within the Internet of Things (IoT) paradigm is discussed. Of the various forms of scanning techniques, fingerprint, iris, and facial have been selected as a security measure. However, the application of retinal scans for security within ATMs in Pakistan is novel. Retinal scans face many issues such as external pressures that can make the implementation of retinal scans difficult, proper technological advancements for implementing of retinal scans, costing and whether it will serve as a barrier and whether the overall concept of implementing retinal scans is a workable idea or not. The sample taken was of 80 close-ended questionnaires filled along with 4 focus group discussions. The questions related to technology, economics and situational awareness concepts. The concept of automated houses and the use of objects with artificial intelligence were of special interest. It is shown that external factors especially cost and technological limitations prohibit widespread adoption of biometric-based retinal scans and implications for overall privacy and security that is present.

Keywords: *Biometric scans, retinal scans, ATMs, IoT*

JEL Classification*: O33*

INTRODUCTION

Automatic Teller Machines (ATMs) users have multiplied over the last few years. It relies on the concept of using ATMs to facilitate banking needs with ease and simplicity. The ATM card is a plastic card that allows the individual to carry out transactions based on different services such as deposits (through the Cash Deposit Machine or CDM), amount transfers, balance checks, cash withdrawals based on certain limits assigned to name a few. Each card has its own set of unique PIN codes that can be applied. This PIN code or password state in layman terms is a four-digit number that is used by the individual as per the verification and authentication of the bank. The aim of the PIN code is to protect the individual during times of theft. If the card is lost or stolen, then it allows the person to gain access to large amounts of funds, for which the PIN provides protection (Jaiswal & Bartere, 2014).

Correspondence:
* *Research Scholar, Institute of Business Management, Karachi. std_19829@iobm.edu.pk*
** *Associate Professor, College of Engineering and Sciences, Institute of Business Management, Karachi. imran.majid@iobm.edu.pk*

New technology has allowed customers to have limited interaction with the bank. It now handles routine transactions through the use of ATMs by most customers; the number of people waiting for service declines. So workloads for tellers have reduced, and it improves their accuracy and quality of service (Ganiyu, Alhassan & Muhammad-Bello, 2015). It is based on the study of ATM facilities and the factors affecting the choice of ATM along with post-purchase behaviour of customers on SBI, ICICI and HDFC (Ganiyu, Alhassan, & Muhammad-Bello, 2015). It has been examined that the customer satisfaction level for problems is highest in SBI. The post-purchase behaviour rating was found to be highest with HDFC Bank (Hota, Nasim, & Mishra, 2013). The average satisfaction level was found to be highest with HDFC Bank. The ATM technology has developed so much that some ATMs can remember consumer preferences as per their previous transactions behaviour and customize services accordingly. Even some ATMs have internet capability which provides two-way interactions with live agents, offer biometric security capability and display personalized advertisements (Hota, Nasim & Mishra, 2013).

Banks are interested in changing software continuously and have consistent behaviour across their networks (Hota J. R., 2012). ATMs perform well if the experience is personalized. Another dimension in ATM technology is the sharing of an ATM network among banks. Studies have shown that no one can gauge the overall impact of business and the positives that can be gained based on the overall application of the ATM network. However, there are certain processes that can be applied which aid in the management of how banks can not only understand but work on the benefits (Hota J. R., 2012). Within the researcher's exploratory work it was found that geography also plays a role as it looks into the ATM network formations of not only urban and local but also between competitive banks. They base the difference that is present here on the application of adopting and applying new technology in banks for developing countries (Hota J. R., 2012). The impact of changing ATM technology on banks provides a different result based on the size of banks, competition based on usage of technology and deployment of ATM networks. In this paper, we look into the trends of biometrics present within ATMs.

STATE OF THE ART TECHNOLOGY

There are many trends that have been identified in the process of ATM security. Looking into the concepts and trends offered, the initial trend noted is that of authentication followed by biometric integration. The authentication process allows the transaction to take place with a code provided by SMS, following suit with the fingerprint scan. Looking into the trends of ATM security the following are observed:

Double Authentication

One of the initial trends that were noted and proposed by Ganiyu et al. (Ganiyu, Alhassan, & Muhammad-Bello, 2015) in the year 2015 was based on double authentication using the aid of a passcode to be shared through the SMS. As per Figure 1 that is the 'Second level authentication model, it is clear that the process of double authentication is based on managing different hardware and software that will be used simultaneously. The model in question shows that there are four key features that will be applied. The first is ATM, second the bank's server, third is SMS facility and last but not the least the fourth is the customer. Here, the SMS facility

is based on the Short Message Application Programming Interface (SMS API) (Ganiyu, Alhassan, & Muhammad-Bello, 2015).

The application of the software for this desired process will be done so with the use of Java or C language in programming. The standard form of managing the database will be used under the name of MySQL. The SMS that will be sent to all customers will be done so with the use of SMS API as per the SMS gateway (Ganiyu, Alhassan, & Muhammad-Bello, 2015).

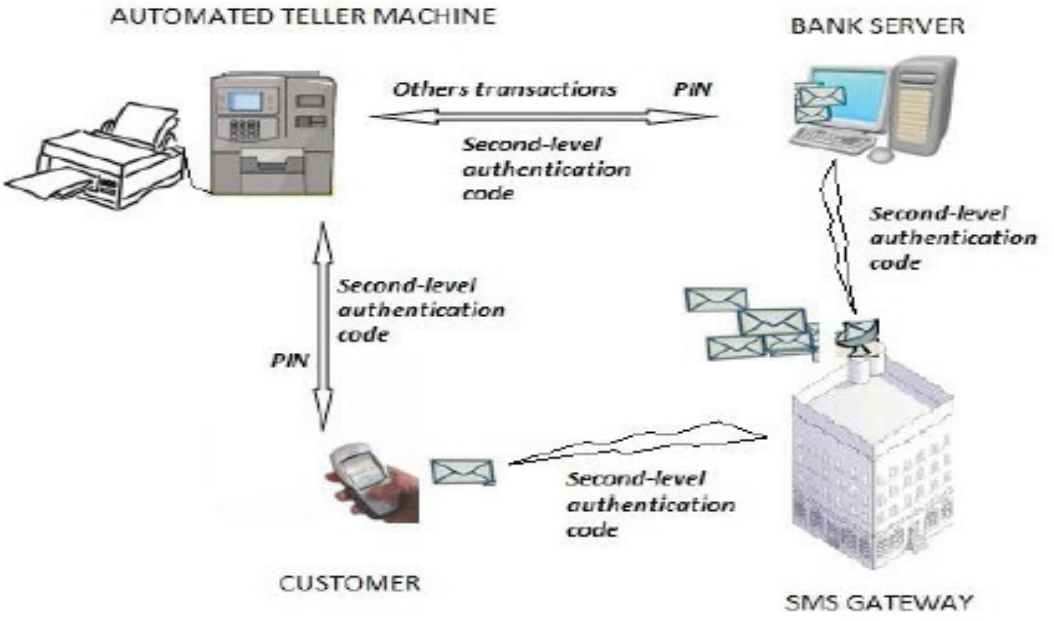

Figure 1. Second-level authentication model (Ganiyu, Alhassan, & Muhammad-Bello, 2015)

Biometrics Integrated with Network Technology in Pakistani Banks

There is different prior work that has taken place allowing the use of biometrics as a security tool within ATMs. Here various applications of Biometrics and GSM (Ganiyu, Alhassan & Muhammad-Bello, 2015) are explored. For understanding the trends around the world of ATM security, the old forms that are based on the use of fingerprint scanning and GSM combined are noted sharing the limitations that have been faced within these forms.

Fingerprint Verification

The concept of ATM fingerprint verification has gained attention. It basis the first on the idea of fingerprint biometric token (Ganiyu, Alhassan & Muhammad-Bello, 2015). The idea is based on having access to accounts within ATMs with the use of fingerprints within the bank's database. Initially, there were two limitations. The first is the database not being developed for fingerprinting. The second was in line to the fact that it couldn't be linked to the actual one (Ganiyu, Alhassan & Muhammad-Bello, 2015; Hota, Nasim & Mishra, 2013).

Moving forward, the remaining work was based on Short Message Service (SMS) verification. They based it on the development of an algorithm for improving the authentication

system of ATMs with the help of text message verification (Oko & Oruh, 2012). The usability testing of the proposed system was conducted with the algorithm only considered using a minimum withdrawal amount. Further, the third party's fingerprint was included in the design (Ravikumar, Vaidyanathan, Thamotharan & Ramakrishan, 2013). One study states that fingerprint biometric and GSM technology proposes an algorithm that provides two phases of security as alternatives (Padmapriya & Prakasam, 2013). For this research, the authors identified no limitations (Padmapriya & Prakasam, 2013). Another study shares a new form of biometrics that is based on the Iris Recognition and Palm Vein (IRPV) recognition technology. It was based on using the Iris Recognition and Palm Vein (IRPV) recognition technology to identity theft and criminalities through an ATM. However, this proposed system was not built as an improvement on the existing system (Das & Debbarma, 2011). Another research presented by Okereke et al. (Okereke, Ihekweaba and Okpara (2013) proposed facial recognition technology. It was a system that incorporated facial recognition technology into the identity verification process used in ATMs. The existing system is not being replaced by the proposed system but merely improves it. The study also relied on a facial recognition program that was open-source and the local features that will be analysed are not being discussed (Santhi & Kumar, 2012).

ATM SCANNING & IoT

There are many ways in which banks can use IoT. We can use information technology to find branch locations, new branches, in-branch services, automating different transactional facilities and potential areas of improvement. More significantly, IoT helps increase the loyalty of a customer by providing personalized services in various sectors other than banks.

IoT and Biometric Scanning

The concept of IoT involves multiple data terminals interconnected in a distributed fashion, where user terminals are allowed transmission and reception of data. IoT is an integrated infrastructure in the financial sector upon which various services and applications run including daily life routines, proficient transportation at a metropolitan level, and worldwide delivery systems (Prithika & Rajalakshmi, 2013).

In an IoT enabled environment, there will be a ubiquitous large amount of data which is accessed collected processed and re-transmitted that convert this metadata into useful knowledge for the end-user. As malware and different attacks become progressive, it requires physical access in a safe and secure manner. It is expected that many real-time data streams exist; that is basic for a stream of information to be utilized in multiple ways to implement privacy and enhance security. The system shall be completely accurate. Uncertainty in data interpretation can cause users to mistrust the system (Prithika & Rajalakshmi, 2013).

Application of IoT in Retinal Scanning

The human retina is a flimsy tissue made of neural cells that are situated in the back segment of the eye. On account of the perplexing structure of the vessels that supply the retina with blood, every individual's retina is unique The system of veins in the retina is complex to where even identical twins don't share a comparable example. Although retinal patterns might be altered in cases of retinal degenerative disorders, glaucoma, or cataracts, the retina usually

remains unchanged throughout the lifespan. Because of its constant nature, the retina gives off an impression of being the exact and dependable biometric. (Okereke, Ihekweaba, & Okpara, 2013). Advocates of retinal scanning have inferred that estimates in its error rate are only one in a million (Okereke et al,. 2013).

Using IoT in retinal scans is easy to go password-less. It allows better security against existing breaches via multi-level security stages. Here, on-the-go monitoring facility improvises and implements security solutions as soon as required (Amin, Chong, Hashim & Chizari, 2015). Compatibility with different platforms and gadgets results in a good response from the customer's end. The customized biometric security features help make distinctive security standards for various purposes. It permits a simpler validation process once we get the biometric data. IoT can be considered a universal solution by allowing the same biometric information to be used for other security applications. The modular isolation of the system from the core operations differentiates malware from creating potential risks (Sagheer, 2012).

IoT is based on confirmation done via a smart device. The IoT based biometric systems can likewise be utilized to verify individual presence. So that individual's location record can be authenticated efficiently. This enables it to have full-time support for better feasibility for implementation. Mapping of biometric information is tough to recreate, as compared to traditional passwords, and it significantly reduces time complexity (Oko & Oruh, 2012).

SYSTEM MODEL

The retina is universal and unique. A consistent property of a retina pattern of a human is that it stays constant. More accurate than any other biometric system, retinal scanning helps prevent identity theft or fraud. Retinal scanners are not subject to dirt or lead to finger impression imprints like fingerprints. Further, they have extremely low false-positive rates (almost 0%). Low occurrence of false negatives is also characteristic. This is because fooling the retinal scanner is very difficult. It is feasible & easy to use. This has led to highly reliable and speedy results. The data that retina scan capture and the store does not occupy too much storage space. We hence consider this an ideal option for IoT integration.

The application of biometric systems deceives the simple process of cryptography. The main purpose of using cryptography here is because it aids in promoting the system in two ways. It offers high and adjustable security measures that can remove the disadvantages of the traditional authentication systems etc. For the application of this process, therefore, a specialized cryptographic key is produced from the biometric layout of a client which is stored in a database. This dedicated key cannot be accessed without the appropriate biometric confirmation system (Stankovic, 2014).

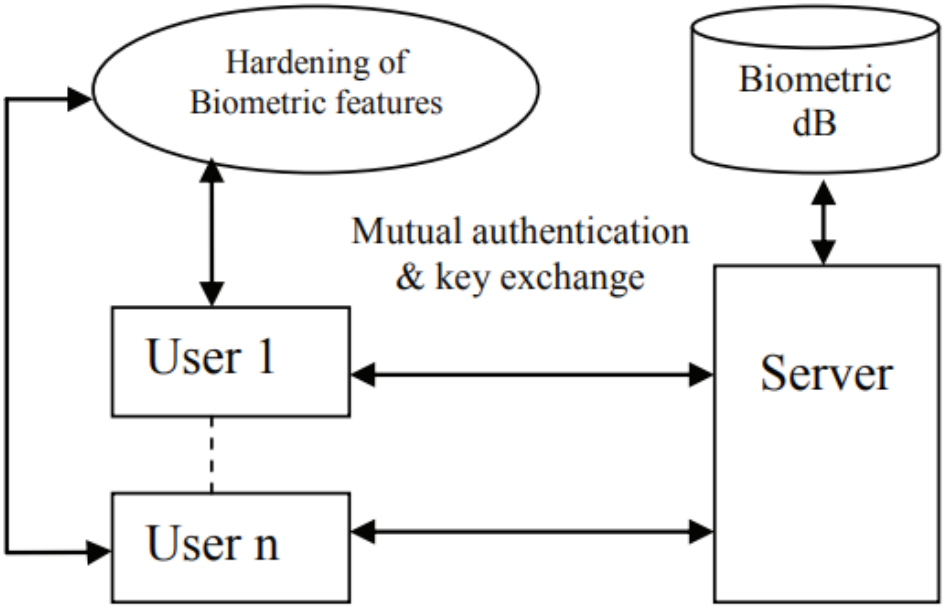

Figure 2. Biometric system & security implementation (Subha, 2017)

A novel method used by Li Chen (Subha, 2017) extracts the configuration of a retina. It carries morphological and thinning actions on the texture of retina. The vascular retinal patterns are emphasized in these operations. The bifurcation characteristic points are then obtained from the vascular designs. The (x, y) coordinates of the retinal bifurcation points are used to create a secret key (Subha, 2017).

The translation and permutation applied to the retinal vascular tree with the bifurcation points highlighted in Fig 3(d) show the pre-transformation feature and Fig. 3(e) shows the feature point for retina after transformation. The exclusive feature points from the original feature points are extracted. The user password is limited to 8 characters with a constraint. The user password is limited to 8 characters with a constraint. Therefore, the password length is 64 bits comprising four 16-bit blocks. The point of emphasis on the iris template and the vascular retinal tree is divided into 4 quadrants. Every quadrant is assigned to a single password block. A permutation is used in such a way that the relative position of the feature point is not changed (Abreu, Santin, Viegas, & Stihler, 2017).

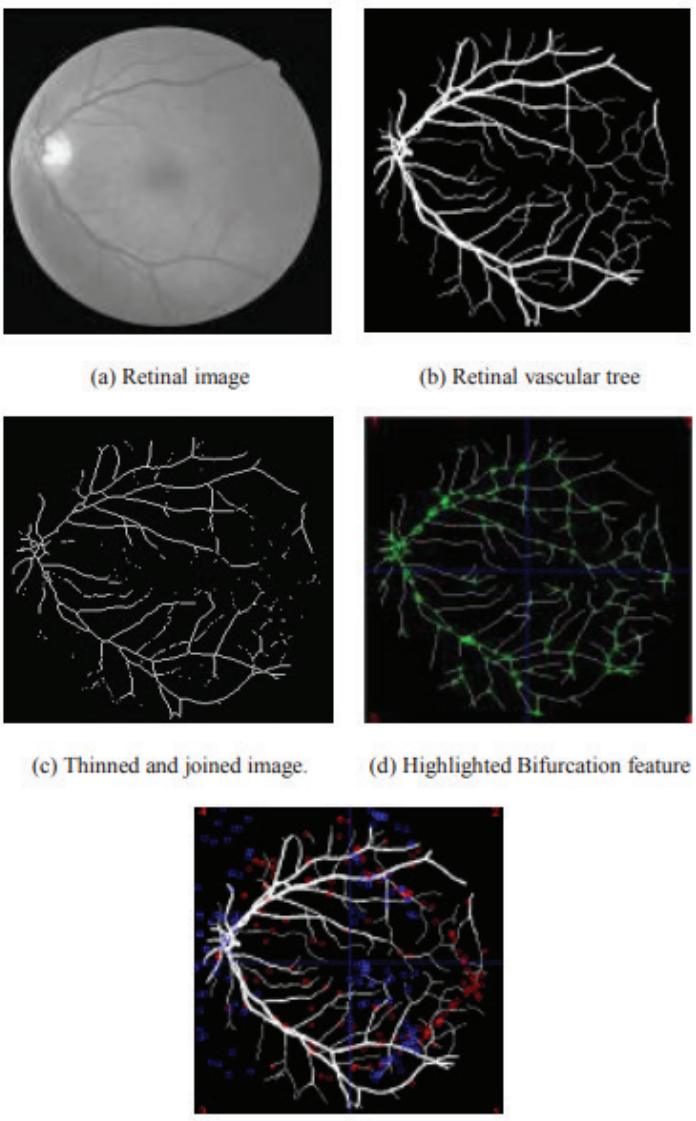

Figure 3. Image process of a retinal scan (Abreu, Santin, Viegas, & Stihler, 2017)

The 16-bit password block is divided into 7 bits Tu and 9 bits, Tv in length. Tu and Tv are longitudinal and latitudinal translations. The new feature points are obtained by the following transformation.

$$X'u=(Xu+ Tu)mod(2^7)$$
$$Y'v=(Yv+ Tv)mod(2^9)$$

X'u and *Xu* represent the horizontal distance between points before and after transformation, respectively while verticals are denoted by*Y'v* and *Yv* respectively. This was applied in case of the human retina (Abreu, Santin, Viegas, & Stihler, 2017).

The transformed features are further encoded. The polynomial for CRC generation is $g_{crc}^{(a)}$

$=a^{16}+a^{15}+a^{2}+1$ (Saraswathi, Jayaram, & Balasubramanian, 2011).

The placement of the Euclidian distance is less than D, which is removed in the combined set. x and y coordinates (every 8 bits) have been concatenated to receiving the 16-bit lock/unlock unit *'u'*. The *'u'* values are sorted and it selects the first N of them. The Secret Code (SC) is partitioned into 16 bits each. The projection of *'u'* on polynomial *'p'* is found. The Genuine points set G is (ui, P(ui)). Random chaff points are produced 10 times in number that of the genuine points. Both the genuine and chaff point sets are combined for the encoding (Saraswathi, Jayaram, & Balasubramanian, 2011).

METHODOLOGY AND SAMPLING

The methodology used here is based on exploratory research with both qualitative and quantitative research. The target audience and population that has been applied is based on individuals belonging to the banking sector from within the region of Karachi. The sample size adopted for conducting the interviews is 80 and focus groups are 4 (with eight individuals in each group). The focus group comprises of 4 individuals (with 8 individuals in each group). An error margin of 11% is assumed and a confidence level of 95% is expected. The data gathered has been tabulated and analysed using the Chi-square formula. The data gathered has been tabulated and analysed with the use of the Chi-square formula, as we need to understand the relationship between two or more unknown parameters.

The hypotheses that have been considered for this paper are:

H_1: External pressures will make the implementation of retinal scans for ATMs difficult for banks.

H_2: Banks do not have the proper technological advancements for the implementation of retinal scans for ATMs.

H_3: The cost of implementing retinal scans for ATMs will be a barrier for banks.

H_4: Retinal scans for ATMs have high-security risks; thus, implementation is not feasible.

Data gathered from qualitative research is based on perceptions that can be derived from the focus groups held. The analysis shows that the banking industry is fast-paced and has over gone many changes. Transactions have moved from the typical depositing a cheque and gaining income, to where transactions are not only carried out through the use of a plastic card but also online. "I remember there was a time when there was a bank called Union Bank and also ANZ Grindleys, but now they both are SCB".

Banks today are subject to a lot of fraud with news splattered about how different hackers gain access and take large sums of money. If not hacking, then simply stealing through the ATM is also there. Most of the respondent's state that stealing through the ATM is easier for people as they have cameras attached that tends to not only look into their PIN codes but also their card information. It seems that only a few people are aware of the fact that upon entering the ATM it is important to check the device and see if there is nothing out of the ordinary on it. "I remember this one ATM is Johar had a false keypad, I didn't use the ATMs in that area

but had to go to blocks ahead to use them".

Biometrics is a form that is recalled by all and sundry. It is the application of a person's physical form that allows the person's identification to occur. The key identification feature is fingerprinting. From the use of fingerprinting in workplaces, ATMs have been introduced that use fingerprinting as well. Different branches have ATMs that offer biometric fingerprint scanning as well to access accounts; however, it is observed that the use of this service is quite limited. Not many are aware of the idea of using fingerprints to gain access to their personal accounts. Those who are aware of this feature know that it is not only safe but simple and easy to follow as well. The implementation of a new biometric feature, if the process is well explained, is considered unique. Retinal scans are considered different and therefore implementation might take time. The process flow that is proposed is shown in the figure below.

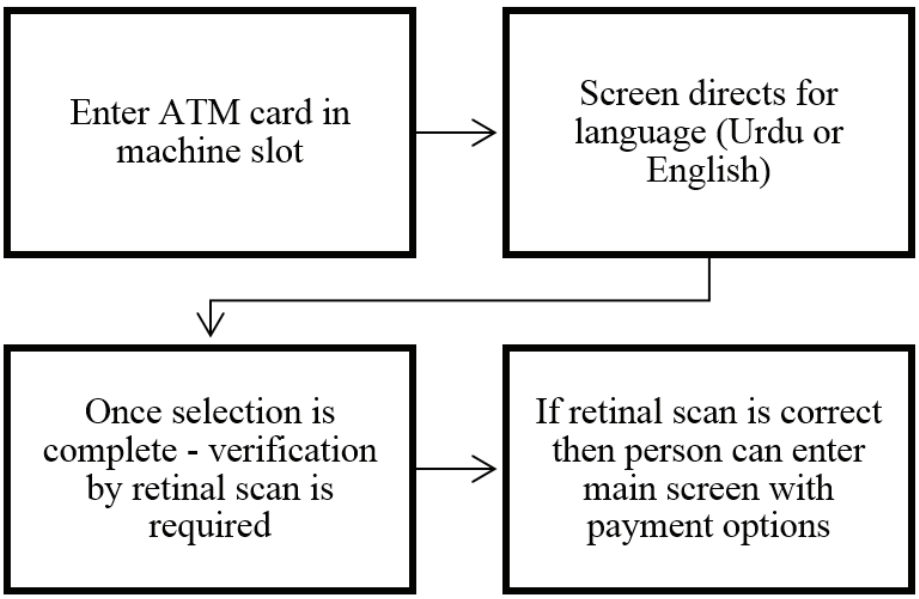

Figure 4. Proposed Flow Chart

On the third stage that is the retinal scan, the process would be:

1. Looking into the camera that has infrared light
2. The camera takes a shot of the retina and sends it to the database.
3. The database tallies the scan and gives confirmation
4. Once a person is verified, the transaction can take place.
5. If a person is not recognized by the database, then the machine cancels the transaction.

The process for recognizing who it is that is making the transaction. This means that during the stage of verification, it needs to verify whether the person is actually the same or not. During this stage, therefore, the problem that can be noted is that whether the person, say Y matches the biometric retinal scan image that has been saved in the database as Ax. Now when the data is run it has to authenticate that (Y, Ax) can be grouped either with the base of B1

or B2. Here, B1 stands for the authenticated user whereas B2 stands for those who couldn't be verified and therefore were considered as false identities. Now when the aspect of matching templates is done here, Ax is to be matched against the corresponding template Ay. The formula that will be developed therefore will be

$$(Y, Az)\ \varepsilon \begin{cases} B1, \text{ if } G\ (Ax, Ay) \geq t \\ B2, \quad \text{otherwise} \end{cases}$$

Here G caters to the scales will be applied to measure and predict the similarity between both Ax and Ay, while t is noted to be the redefined threshold. Therefore S(Ax, Ay) can be taken as the scores to create the perfect match. It is noted that the field of biometrics, being a part of science is constantly evolving. Therefore, when looking into the banking sector, if one bank brings something new, others will soon follow suit for sure. There are many forms of verifications that can be added in ATMs such as:

- Facial
- Iris
- Retinal

Others such as that of voice and signature seem invalid and there is no way of matching voice nodes to that of account codes as per the perception of the respondents. The facial scan allows a camera to identify the face of the person, highlight the main verification features and thus allow the person to gain access to their accounts. Iris scanning again involves the application of a camera that allows the image of the iris to be captured and used for identification by linking it to the account. The last was that of the retinal scan. This process applied the infrared light that allows the identification of a person's unique vein patterns and once recognized allows them access.

The concept of facial and iris scans was relayed and recalled from not only the use of mobile phones but also security for high risk or high-security areas. Thus, the concept of retinal scans was thought of as more unique and therefore was discussed and shared below.

RESULTS AND ANALYSIS

The data that has been gathered for the hypothesis is shared below with the application of the Chi-square test. For each hypothesis, the data has been presented in the form of observed and expected. Data for Table 1 to Table 8 were gathered from the questionnaire appended at the end.

> ***H_1:*** External pressures will make the implementation of retinal scans for ATMs difficult for banks.

The hypothesis looks at the external pressures on implementing retinal scans in ATMs. Therefore, it looks into external factors such as competition (C), Politics (P), Environment (E) and Social factors (S). Yes, implies to the state that external pressures will impact the implementation of retinal scans, while no states that it won't. The observed results are as follows:

Table 1: Observed results for external sources

	C	P	E	S	TOTAL
Yes	*45*	*12*	*11*	*8*	*73*
No	*0*	*1*	*2*	*4*	*7*
TOTAL	*45*	*13*	*13*	*12*	*80*

The expected results are as follows:

Table 2: Expected results for external sources

	C	P	E	S	TOTAL
Yes	*41.1*	*11.9*	*11.9*	*10.9*	*73*
No	*3.9*	*1.1*	*1.1*	*0.8*	*7*
TOTAL	*45*	*13*	*13*	*10*	*80*

Formula applied: $X^2 = \frac{(O - E)^2}{E}$

Therefore, the Chi-square here is =

$$X^2 = \frac{(45 - 41.1)^2}{41.1} + \frac{(13 - 11.9)^2}{11.9} + \frac{(11 - 11.9)^2}{11.9} + \frac{(8 - 10.9)^2}{9.1} = 14.94$$

The degree of freedom at 2 with a level of (.05), the table shows the cut-off at a 14.9 score.

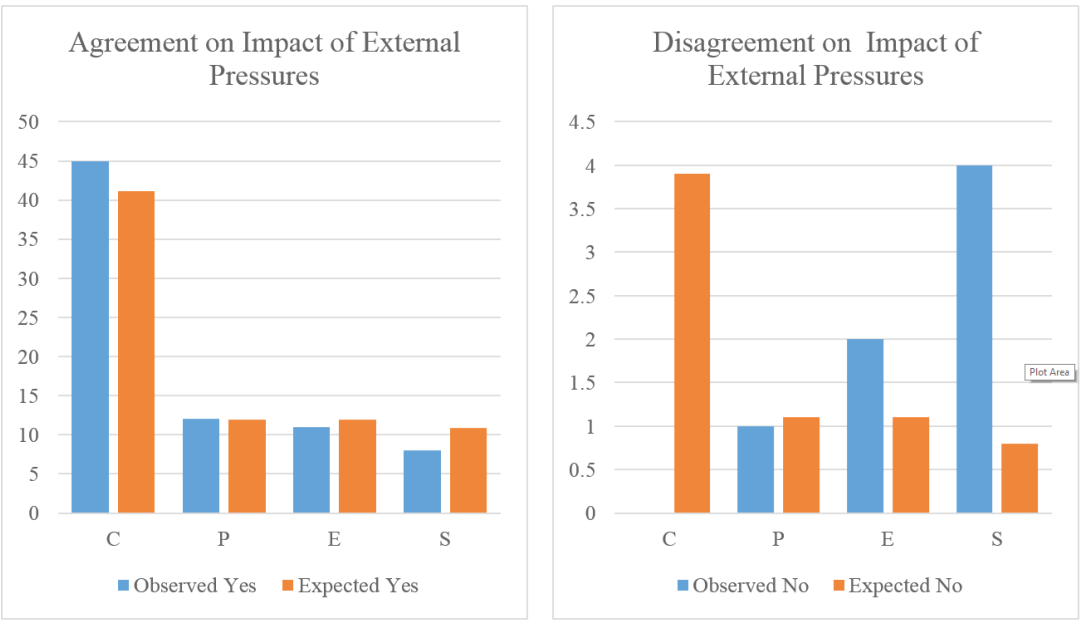

Figure 5. Comparison between Observed and Expected Response on the Impact of External Pressures

The results indicated that people perceived the competition not only to be more significant on external pressure but also very deviated from the expected results. This was probably due

to the fact that the general public is aware of society's inclination toward change and how technology is resisted in general. People will most probably oppose the use of retinal scans as the competition with respect to other biometrics is very high. Pin codes and fingerprint scans are considered as sufficient authentication technique for ATMs. These go in parallel with the social factor too. The politics of the country and environmental factor are not noteworthy as the authentication technology does not directly affect either of them.

> ***H_2:*** Banks do not have the proper technological advancements for the implementation of retinal scans for ATMs.

The hypothesis looks at whether banks do not have the proper technological advancements for retinal scans in ATMs. The observed results are as follows:

Table 3: Observed results for technological advances

	Complete technological advancements	**Incomplete technological advancements**	**TOTAL**
Agree	*27*	*23*	*50*
Disagree	*10*	*20*	*30*
TOTAL	*37*	*43*	*80*

The expected results are as follows:

Table 4: Expected results for technological advances

	Complete technological advancements	**Incomplete technological advancements**	**TOTAL**
Agree	*23.1*	*26.8*	*50*
Disagree	*13.9*	*16.2*	*30*
TOTAL	*37*	*43*	*80*

Formula applied: $X^2 = \frac{(O - E)^2}{E}$

Therefore, the Chi-square here is =

$$X^2 = \frac{(27 - 23.1)^2}{23.2} + \frac{(10 - 13.9)^2}{13.9} + \frac{(23 - 26.8)^2}{26.8} + \frac{(20 - 16.2)^2}{16.1} = 3.16$$

The degree of freedom at 2 with a level of (.05), the table shows the cutoff at a 3.84 score.

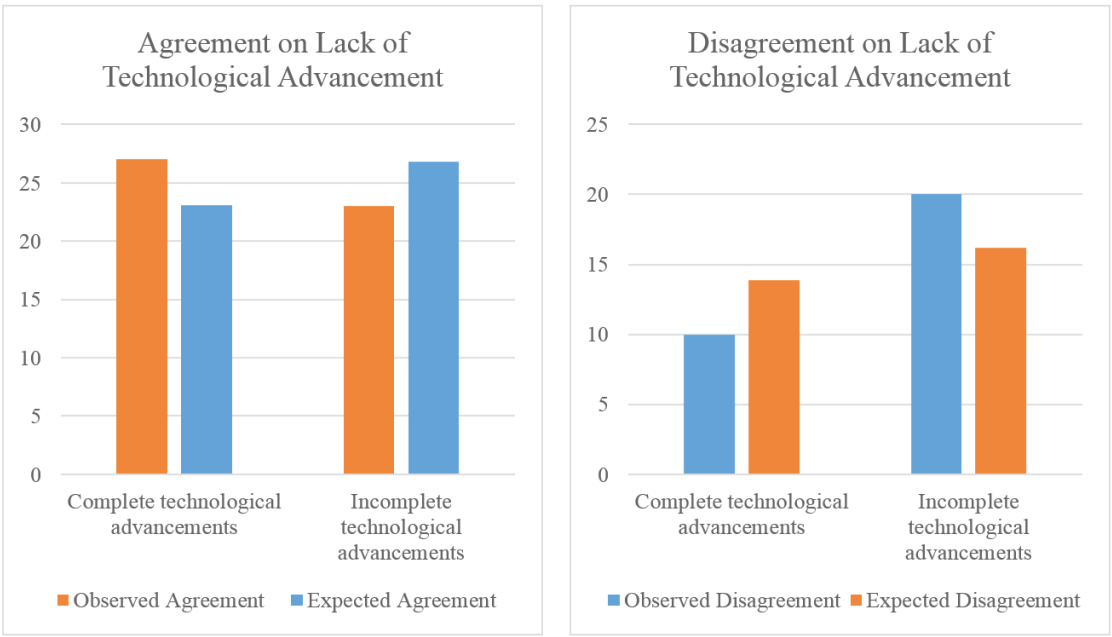

Figure 6. Comparison between Observed and Expected Response on Lack of Technological Advancements

Being a third world country, Pakistan is far behind in technological advancements which directly related to the unease of end-users adapting to new technology. Although the expected result was likely for disagreement over lack of technological advancement, the result turned out to be opposite. The viewpoint of the general public usually does not cater to the infrastructure behind the implementation of technology and expertise required. But the results of the survey suggest that people are confident that the country is sufficient in technology when it comes to retinal scans.

H_3: The cost of implementing retinal scans for ATMs will be a barrier for banks.

The hypothesis looks at whether the cost of implementation for retinal scans in ATMs will serve as a barrier. The observed results are as follows:

Table 5: Observed results for costing of retinal scans

	High cost	**Low cost**	**TOTAL**
Agree	*27*	*21*	*48*
Disagree	*17*	*15*	*32*
TOTAL	*44*	*36*	*80*

The expected results are as follows:

Table 6: Expected results for the costing of retinal scans

	High cost	**Low cost**	**TOTAL**
Agree	*26.4*	*21.6*	*48*
Disagree	*17.6*	*14.4*	*32*
TOTAL	*44*	*36*	*80*

Formula applied: $X^2 = \frac{(O - E)^2}{E}$

Therefore, the Chi-square here is =

$$X^2 = \frac{(27 - 26.4)^2}{26.4} + \frac{(21 - 21.6)^2}{21.6} + \frac{(17 - 17.6)^2}{17.6} + \frac{(15 - 14.4)^2}{14.4} = 0.06$$

The degree of freedom at 2 with a level of (.05), the table shows the cut off at a 0.06 score

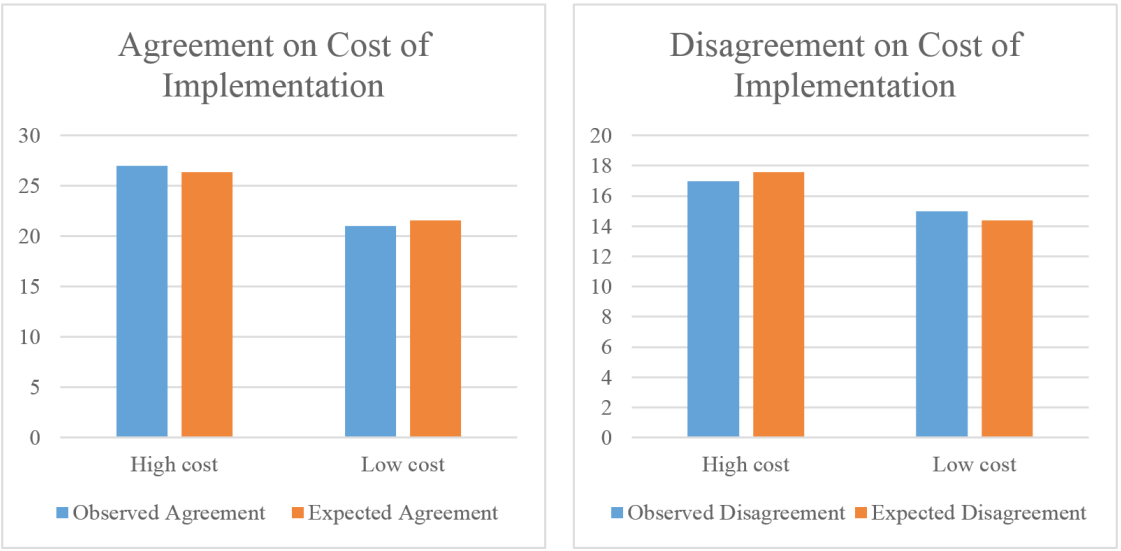

Figure 7. Comparison between Observed and Expected Response on Cost of Implementation

The results of the survey pertaining to implementation cost are very close to our expected results. These include the cost of integrating new technology in an existing system, cost of additional hardware, and retina registration cost.

> ***H_4:*** Retinal scans for ATMs have high-security risks, thus the implementation is not feasible.

The hypothesis looks at whether implementing of retinal scans would be considered as feasibly secure. The observed results are as follows:

Table 7: Observed results for the feasibility of retinal scans

	High Feasibility	**Low Feasibility**	**TOTAL**
Agree	*31*	*12*	*43*
Disagree	*11*	*26*	*37*
TOTAL	*42*	*38*	*80*

The expected results are as follows:

Table 8: Expected results for the feasibility of retinal scans

	High Feasibility	Low Feasibility	TOTAL
Agree	*22.6*	*20.4*	*43*
Disagree	*19.4*	*17.6*	*37*
TOTAL	*42*	*38*	*80*

Formula applied: $X^2 = \frac{(O - E)^2}{E}$

Therefore, the Chi-square here is =

$$X^2 = \frac{(31 - 22.6)^2}{22.6} + \frac{(12 - 20.4)^2}{20.4} + \frac{(11 - 19.4)^2}{19.4} + \frac{(26 - 17.6)^2}{17.6} = 14.1$$

The degree of freedom at 2 with a level of (.05), the table shows the cut-off at a 14.1 score.

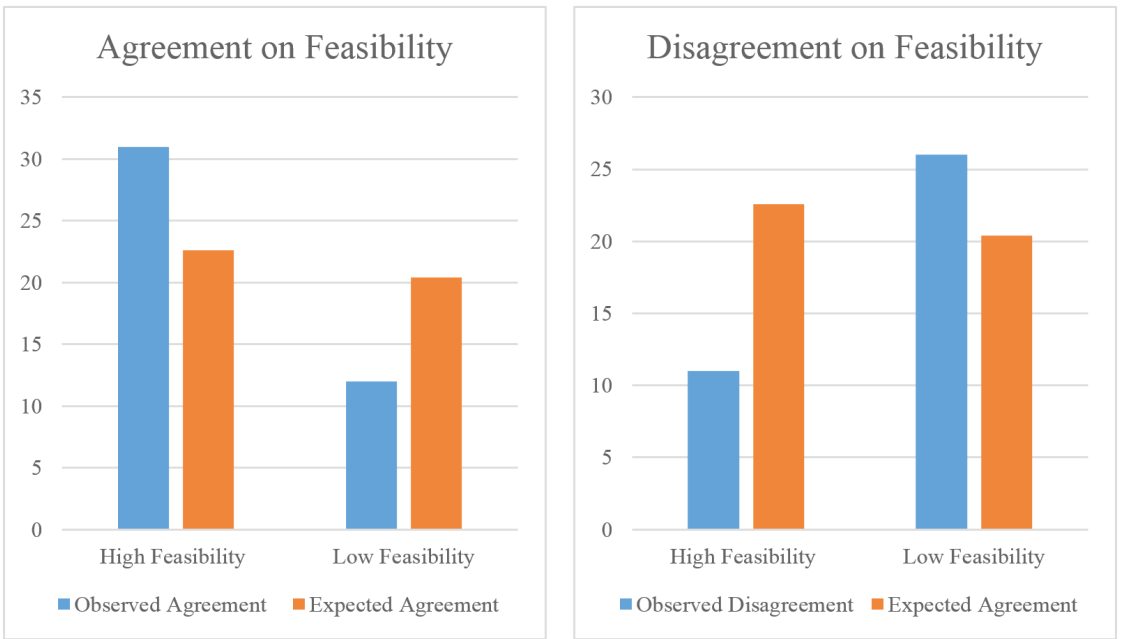

Figure 8. Comparison between Observed and Expected Response on FeasibilityUnfavourable Budget

Figure 8. Comparison between Observed and Expected Response on Feasibility

Feasibility of any system, when discussing among the general public, usually gives off a different vibe. Each person has his own opinion on the practicality of a new system over the existing one. The educated guess on both the agreement and the disagreement usually deviates from the actual results as interviewee links personal experiences and compatibility with both new and old technology. People find it more feasible for the retinal scans to be used for authentication purposes.

CONCLUSION

WE can consider ATMs as a technology that is not only mature but also offers financial services and ease of security to people in different locations of the world. Using fingerprint scanning and GSM integration has made life simpler and more convenient. The conclusion from the above case study helps to appreciate that technological hurdles and the cost of retinal scans are the predominant factors that prevent its adoption. Further, application of IoT has also managed to enhance this at an even bigger scale. The new concept is to be introduced for retinal scans has major potential: The idea is feasible, given the cost and data development are optimized and further researched.

LIMITATIONS

Looking at the concept of having retinal scans, the idea is used in most-high security zones such as government organizations and crime management firms. The idea of biometric scans is not old. Many companies have adopted this concept and have used fingerprinting to enable their employee's entry or exit. The fingerprint scan is not just for entry or exit, it aids in verifying and identifying the person and validating whether they are who they claim to be. As has been stated, fingerprinting is now used in ATMs as well. People can easily access their accounts and withdraw money by using their fingerprints. With though this idea is secure and safe there are many ways where the fingerprint scans can be replicated and copied. Therefore, the retinal scan is a concept that can be used in ATMs. The idea does have limitations.

One factor that can serve as a limitation is that there has to be a proper framework in place for database protection. They have to be monitored at all times and have to be under proper security so that no hackers can have access to it. Maintaining such protocols also has a cost. This leads to the other limitation of financial costs. The more complex the technology the higher the cost perceived. Not only this, the cost of managing and maintaining the overall database system be high as well. All this has to be processed and worked upon so that there are neither ambiguities in data nor any loopholes present to create issues.

REFERENCES

Abreu, V., Santin, A. O., Viegas, E. K., & Stihler, M. (2017). A multi-domain role activation model . *Communications (ICC) 2017 IEEE International Conference,* 1-6 . doi:ISSN 1938-1883.

Amin, N. F., Chong, S. E., Hashim, N. Z., & Chizari, H. (2015). Security Issues in ATM Smart Card Technology. *International Journal of Mathematics and Computational Science, 1*(4), 199-205.

Das, S. S., & Debbarma, S. J. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. *International Journal of Information and Communication Technology Research, 1*(5), 197-203.

Ganiyu, S. O., Alhassan, M. E., & Muhammad-Bello, B. L. (2015). An Enhanced ATM Security System using Second-Level Authentication. *International Journal of Computer Applications, 111*(5), 8 - 15.

Hota, J. R. (2012). Windows Based and Web Enabled ATMs: Issues and Scopes. *IUP Journal of Information Technology, 8*(4), 52-59.

Hota, J., Nasim, S., & Mishra, S. (2013). Automated Teller Machines in India: A Literature Review from Key Stakeholders Perspectives. *Department of Management Studies, 1*(1), 1086 - 1105.

Jaiswal, A. M., & Bartere, M. (2014). Enhancing ATM Security Using Fingerprint and GSM Technology. *International Journal of Computer Science and Mobile Computing (IJCSMC), 3*(4), 28 – 32.

Okereke, E., Ihekweaba, G., & Okpara, F. K. (2013). Facial verification technology for use in ATM transactions. *American Journal of Engineering Research (AJER), 2*(5), 188-193.

Oko, S., & Oruh, J. (2012). Enhanced ATM security system using biometrics. *IJCSI International Journal of Computer Science Issues, 9(*5(3)), 352-357.

Padmapriya, V., & Prakasam, S. (2013). Enhancing ATM security using fingerprint and GSM technology. *International Journal of Computer Applications, 80*(16), 43-46.

Prithika, M., & Rajalakshmi, P. (2013). Card duplication and crime prevention using biometrics. *IOSR Journal of Computer Engineering (IOSR-JCE), 10*(1), 1-7.

Ravikumar, S., Vaidyanathan, S., Thamotharan, S., & Ramakrishan, S. (2013). A new business model for ATM transaction security using fingerprint recognition. *International Journal of Engineering and Technology (IJET), 5*(3), 2041-2047.

Sagheer, A. M. (2012). Elliptic curves cryptographic techniques. *Signal Processing and Communication Systems (ICSPCS)*. International Conference on. IEEE.

Santhi, B., & Kumar, K. R. (2012). Novel hybrid technology in ATM security using biometrics. *Journal of Theoretical and Applied Information Technology, 37*(2), 217-223.

Saraswathi, K., Jayaram, B., & Balasubramanian, R. (2011). Retinal Biometrics based Authentication and Key Exchange System. *International Journal of Computer Applications, 19*(1), 1-7.

Stankovic, J. A. (2014). Research Directions for the Internet of Things. Life Fellow, IEEE.

Subha, R. (2017). Biometrics in Internet of Things (IoT) Security. *International Journal of Engineering Research and General Science, 5*(5), 37 - 42.